Journal of Computing and Security

April 2015, Volume 2, Number 2 (pp. 109–117)

http://www.jcomsec.org

Robust Cooperative Spectrum Sensing under Primary User Emulation Attack in Cognitive Radio Networks

Abbas Ali Sharifi [a,*], Javad Musevi Niya [b]

[a] *Department of Electrical Engineering, Bonab Branch, Islamic Azad University, Bonab, Iran.*
[b] *Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran.*

ARTICLE INFO.

Article history:
Received: 31 May 2015
Revised: 18 December 2015
Accepted: 16 January 2015
Published Online: 08 May 2016

Keywords:
Attack Parameters, Cognitive Radio, Spectrum Sensing, Primary User Emulation Attack

ABSTRACT

Cooperative Spectrum Sensing (CSS) is an effective approach to improve the detection performance of vacant frequency bands in Cognitive Radio (CR) networks. The CSS process imposes some security threats to the CR networks. One of these common threats is Primary User Emulation Attack (PUEA). In PUEA, some malicious users try to mimic primary signal characteristics and deceive CR users to prevent them from accessing the vacant frequency bands. The present study introduces a new CSS scheme, in the presence of a malicious PUEA, called Attack-aware CSS (ACSS). The idea is based on the estimation of attack parameters including probabilities of the fake PUEA signals' presence in both occupied and unoccupied frequency bands. The obtained parameters are innovatively applied in Neyman-Pearson (N-P) or Log-Likelihood Ratio Test (LLRT) to improve collaborative sensing performance. Simulation results verify the performance improvement of the proposed method against PUEA compared with conventional method.

1 Introduction

Cognitive Radio (CR) has been widely adopted as a promising technology to overcome the spectrum scarcity by authorizing CR users to operate opportunistically in the free space of the licensed frequency bands in co-existence with the Primary Users (PUs) [1]. Spectrum sensing, with the aim of finding the idle frequency bands (spectrum holes), is the main function of CR networks [2, 3]. Collaborative Spectrum Sensing (CSS) is known as an effective approach to improve the detection performance [4, 5]. Unfortunately, spectrum sensing process is vulnerable to Primary User Emulation Attack (PUEA) [6]. In this particular type of attack, malicious user sends signal similar to that of PU transmitter and causes the CR users to immediately relinquish the desired frequency band [6]. To mitigate the problem of PUEA, many approaches have been proposed.

In [7], an analytical model of the PUEA is proposed and a lower bound on the probability of a successful attack is achieved. The authors showed that the probability of a successful PUEA increases with the distance between the CR users and PU transmitter. In [8], a Received Signal Strength (RSS)-based localization defense strategy under the PUEA is proposed to determine the location of PUEA by deploying a sensor network. The authors assume that the PU transmitter is a TV tower with location known to CR users. In contrary, to avoid the deployment of additional sensor networks and expensive hardware in the network, another RSS-based defense strategy against the PUEA

[*] Corresponding author.

Email addresses: a.tabrizu@gmail.com (A. A. Sharifi), niya@tabrizu.ac.ir (J. M. Niya)

ISSN: 2322-4460 © 2015 JComSec. All rights reserved.

is proposed in [9]. In the absence of PU signal, the malicious PUEA sends a fake signal. When the CR users receive the signal, they conduct local spectrum sensing and then use belief propagation to exchange the measurements to detect whether the signal is from a licensed PU or not. Then they exchange information with the neighboring users and calculate the beliefs until convergence. Collaborative sensing in the presence of PUEA is investigated in [10], where the Fusion Center (FC) assigns an appropriate weight to each CR user's sensing measurement and then combines them to maximize detection probability in Neyman-Pearson (N-P) test. The PUEA is assumed to be always present which means the attacker consumes a constant power in all time intervals to defraud the CR users. This strategy is in contradiction with the true definition of PUEA. The authors also analyzed the effect of the channel estimation errors on the cooperative sensing performance. In [11], we consider an intelligent PUEA which is aware of the vacant frequency bands and exactly co-located with the licensed PU transmitter and transmits with the same power level. We obtain the channel occupancy rate of the PUEA and apply in N-P criterion to enhance the collaborative sensing performance. We also introduce an attack-aware threshold selection approach in [12]. The attack parameters are estimated and are used to obtain the optimal thresholds that minimize the global error probability. We show that the proposed method significantly improve the CSS performance under a greedy PUEA. In [13], the authors introduce a smart PUE attacker which is aware of the PU activity and performs spectrum sensing and sends the fake signal with the desired signal occurrence over a special frequency band. They show that the smart attacker has more destructive effect on CSS than the always present one. The authors also investigated the smart PUEA in [14] which applies a target destructive strategy according to its obtained analysis of the radio environment. They also identified possible threats and investigated more efficient and empirical strategies implemented by attackers, finally, they proposed a resilient solution to overcome the attack.

Most of the previous studies to defend against PUEA have been conducted based on assuming that the physical location or unique properties of the PU transmitter is known for CR users or the FC. However, in the presence of a malicious PUEA with unknown location and the same signal characteristics as that of the PU signal, a robust defense scheme is extremely important. Therefore, we propose a new method that does not require any prior information about the location and the properties of the PUEA signal. First, each CR user performs its spectrum sensing and sends its results to the FC. Then, the mean and the second-order moment values of sensing reports are calculated and two attack parameters are innovatively estimated. Two obtained attack parameters include the channel occupancy rates of malicious PUEA in both the presence and the absence of the licensed PU signal. In contrast to [12], in this study the obtained values are hierarchically applied in Log-Likelihood Ratio Test (LLRT) method to improve the collaborative sensing performance. We generalize our initial results in [11]. More precisely, in [11], the PUEA signal occurrence in the presence of the PU signal was considered equal to zero. Here, we assume that the PUEA transmit the fake signal in both vacant and occupied primary bands. The proposed method is called Attack-aware CSS (ACSS) throughout the study.

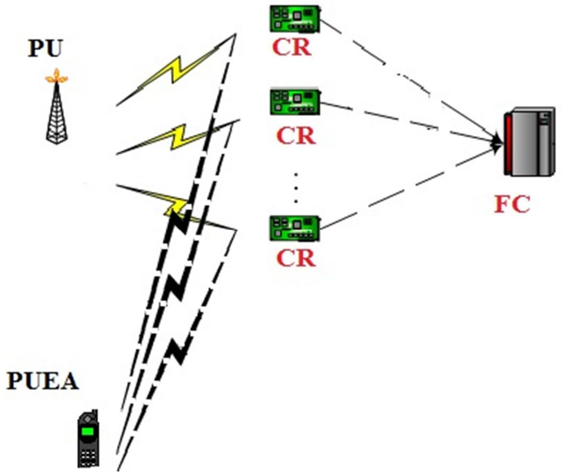

Figure 1. Network Layout

2 System Model

The considered system model is a centralized CR network including a PU transmitter, N collaborative CR users, an FC and a malicious PUEA. It is further assumed that N CR users are randomly deployed in a small area and are geographically far from the PU and PUEA transmitters. The network model is shown in Figure 1.

We assume that the energy detection scheme is used for local spectrum sensing. A malicious PUEA is present in the radio environment which tries to prevent the CR users from accessing the spectrum holes. We further assume a perfect spectrum sensing by the PUEA, i. e, the attacker is able to exactly distinguish between occupied and unoccupied frequency bands allocated to the PU.

Depending on the presence or absence of the PU and PUEA, there are four possible states which can be expressed as:

$$\begin{cases} H_{s0} : onlyNoise \\ H_{s1} : PU + Noise \\ H_{s2} : PUEA + Noise \\ H_{s3} : PA + PUEA + Noise \end{cases}$$

The first state H_{s0} occurs when the CR users receive only noise. Moreover, the channel is neither occupied by PU nor by PUEA. The second state H_{s1} happens when the PU transmits over the channel while the PUEA is absent. If the PU is absent and PUEA transmits the fake signal, the CR users receive only the PUEA signal plus noise, as stated by the third hypothesis H_{s2}. Finally, the last state H_{s3} indicates the simultaneous presence of both PU and PUEA signals.

We assume that two hypotheses H_1 and H_0 indicate the presence and absence of PU signal, respectively. Similarly, the presence and absence of the PUEA signal are denoted by E^{on} and E^{off} , respectively. Based on the above mentioned assumptions, the probability of each hypothesis H_{sk} , denoted by π_k, is determined as

$$\begin{aligned} \pi_0 &= P(H_{s0}) = P(H_0, E^{off}) = P(E^{off}|H_0)P(H_0) \\ \pi_1 &= P(H_{s1}) = P(H_1, E^{off}) = P(E^{off}|H_1)P(H_1) \\ \pi_2 &= P(H_{s2}) = P(H_0, E^{on}) = P(E^{on}|H_0)P(H_0) \\ \pi_3 &= P(H_{s3}) = P(H_1, E^{on}) = P(E^{on}|H_1)P(H_1) \end{aligned} \tag{1}$$

Let two parameters α and β be the conditional probabilities regarding the presence of the fake PUEA signals in two hypotheses H_1 and H_0 , respectively (i.e. $\alpha = P(E^{on}H_1)$ and $\beta = P(E^{on}H_0)$), which are related to attacker strategy. Then, the above equations can be simplified to:

$$\begin{aligned} \pi_0 &= (1-\beta)P(H_0) \\ \pi_1 &= (1-\alpha)P(H_1) \\ \pi_2 &= \beta P(H_0) \\ \pi_3 &= \alpha P(H_1) \end{aligned} \tag{2}$$

By considering the four-level hypotheses, the received signal at the ith sample of the jth CR user, x_j^i , can be formulated as [15],

$$x_j^i = \begin{cases} n_j^i & H_{s0} \\ \sqrt{\gamma_j} p_j^i + n_j^i & H_{s1} \\ \sqrt{\lambda_j} e_j^i + n_j^i & H_{s2} \\ \sqrt{\gamma_j} p_j^i + \sqrt{\lambda_j} e_j^i + n_j^i & H_{s3} \end{cases} \tag{3}$$

where n_j^i is the Additive White Gaussian Noise (AWGN) at the jth CR user. The parameters $\sqrt{\gamma_j} p_j^i$ and $\sqrt{\lambda_j} e_j^i$ are the received PU and PUEA signal with the powers γ_j and λ_j , respectively. We assume that the noise at each sample (n_j^i), the PU signal (p_j^i), and PUEA signal sample (e_j^i) are independently and identically distributed Gaussian random variables with zero mean and unit variance. We further assume that the CR users experience independent block Rayleigh fading channels with the same average SNRs. This condition is relevant for the CR network which is geographically far from the PU and PUEA transmitters. Thus,γ_j and λ_j vary from (observation) period to period while their Probability Density Functions (PDFs) are exponential distributions with the averages of γ and λ , respectively. The parameter $\rho = \lambda / \gamma$ is also defined as attack strength. Obviously, a larger value of $\rho (\rho \gg 1)$ indicates a more powerful PUEA. As mentioned in Equation (3) and with regard to the above assumptions, the received signal, x_j^i , has a Gaussian distribution as [15],

$$x_j^i \sim \begin{cases} N(0,1) & H_{s0} \\ N(0, \gamma_j + 1) & H_{s1} \\ N(0, \lambda_j + 1) & H_{s2} \\ N(0, \gamma_j + \lambda_j + 1) & H_{s3} \end{cases} \tag{4}$$

Moreover, M samples are utilized for local energy detection at each CR user [16, 17]. The observed energy of the jth user, E_j , is given by:

$$E_j = \sum_{i=1}^{M} |x_j^i|^2 \sim \begin{cases} a_j & H_{s0} \\ (\gamma_j + 1) b_j & H_{s1} \\ (\lambda_j + 1) c_j & H_{s2} \\ (\gamma_j + \lambda_j + 1) d_j & H_{s3} \end{cases} \tag{5}$$

where the random variables a_j, b_j, c_j and d_j follow a central Chi-square distribution with M degree of freedom. However, according to central limit theorem [17, 18], if a large number of samples are considered ($i.e.\ M > 10$), E_j can be assumed to have a Gaussian distribution as:

$$E_j \sim \begin{cases} N(M, 2M) & H_{s0} \\ N(M(\gamma_j + 1), 2M(\gamma_j + 1)^2) & H_{s1} \\ N(M(\lambda_j + 1), 2M(\lambda_j + 1)^2) & H_{s2} \\ N(M(\gamma_j + \lambda_j + 1), 2M(\gamma_j + \lambda_j + 1)^2) & H_{s3} \end{cases} \tag{6}$$

In CSS, the locally measured energy of each CR user is sent to the FC to make a global decision about presence or absence of the PU signal. In conventional Equal Gain Combining (EGC) scheme [15], in the absence of the PUEA, all of the sensing reports are summed up and compared with a predefined threshold. If the sum of reports is greater than the threshold then the channel status is determined to be occupied; otherwise, the frequency band is assumed to be idle. The output signal at the FC is:

$$Y = \sum_{j=1}^{N} E_j \underset{H_0}{\overset{H_1}{\gtrless}} \eta_0 \tag{7}$$

where η_0 is the global threshold and determined by the target false alarm or miss detection probability. Obviously, the decision statistic Y has a Gaussian distribution and in the presence of the PUEA, it can be defined as:

$$Y \sim \begin{cases} N(\mu_0, \sigma_0^2) & H_{s0} \\ N(\mu_1, \sigma_1^2) & H_{s1} \\ N(\mu_2, \sigma_2^2) & H_{s2} \\ N(\mu_3, \sigma_3^2) & H_{s3} \end{cases} \tag{8}$$

where one can easily verify that:

$$\begin{aligned} &\mu_0 = MN, && \sigma_0^2 = 2MN \\ &\mu_1 = MN(\bar{\gamma}+1), && \sigma_1^2 = 2MN(\bar{\gamma}+1)^2 \\ &\mu_2 = MN(\bar{\lambda}+1), && \sigma_1^2 = 2MN(\bar{\lambda}+1)^2 \\ &\mu_3 = MN(\bar{\gamma}+\bar{\lambda}+1), && \sigma_1^2 = 2MN(\bar{\gamma}+\bar{\lambda}+1)^2 \end{aligned} \tag{9}$$

For making a final decision about the presence or absence of the PU signal, the Neyman-Pearson (N-P) lemma is used. Assuming that the SNR values are known, the N-P criterionon gives the optimal fusion rule where the criterion is to maximize detection probability with a restriction of false alarm probability [19]. The N-P test compares the likelihood ratio or log-likelihood ratio function (here, we use the second one) defined as follows:

$$\Lambda = log\left(\frac{p(Y|H_1)}{p(Y|H_0)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \eta \tag{10}$$

where the threshold value η is specified by the acceptable false alarm or miss detection probability. Since we assumed that the received energies from different CR users are independent and have normal distribution, we can rewrite Equation (10) as:

$$\Lambda = \left[log\left(\frac{\sigma_0}{\sigma_1}\right) + \left(\frac{(Y-\mu_0)^2}{2\sigma_0^2} - \frac{(Y-\mu_1)^2}{2\sigma_1^2}\right)\right] \underset{H_0}{\overset{H_1}{\gtrless}} \eta \tag{11}$$

Let Q_{fa} be the probability of global false alarm in CSS. Then we have

$$\begin{aligned} Q_{fa} &= P(D^{on}|H_0) \\ &= P(D^{on}|H_0, E^{on})P(E^{on}|H_0) \\ &\quad + P(D^{on}|H_0, E^{off})P(E^{off}|H_0) \\ &= P(D^{on}|H_{s_2})\beta + P(D^{on}|H_{s_0})(1-\beta) \end{aligned} \tag{12}$$

The probability of global detection, denoted by Q_d, is defined as:

$$\begin{aligned} Q_d &= P(D^{on}|H_1) \\ &= P(D^{on}|H_1, E^{on})P(E^{on}|H_1) \\ &\quad + P(D^{on}|H_1, E^{off})P(E^{off}|H_1) \\ &= P(D^{on}|H_{s_3})\alpha + P(D^{on}|H_{s_1})(1-\alpha) \end{aligned} \tag{13}$$

where D^{on} means that the FC's decision is the presence of PU signal.

To evaluate the performance of CSS in the presence of a malicious PUEA and compare it to conventional energy detection, in which the PUEA is not considered, we use correct sensing probability Q_c . The parameter Q_c defines probability of making a correct decision in PU detection. The probability of correct sensing can be written, in general, as:

$$\begin{aligned} Q_c &= P(H_0, D^{off}) + P(H_1, D^{on}) \\ &= P(H_0)(1-Q_{fa}) + P(H_1)Q_d \end{aligned} \tag{14}$$

where D^{off} means that the FC's decision is the absence of PU signal.

With regard to Equations (12) and (13), the above equation can be rewritten as:

$$\begin{aligned} Q_c &= P(D^{off}|H_{s_0})\pi_0 + P(D^{off}|H_{s_2})\pi_2 \\ &\quad + P(D^{on}|H_{s_1})\pi_1 + P(D^{on}|H_{s_3})\pi_3 \end{aligned} \tag{15}$$

In the following section, the proposed ACSS method is thoroughly described.

3 The Proposed Attack-Aware Cooperative Spectrum Sensing

The proposed scheme includes estimation of attack parameters and application of the obtained parameters in the LLRT method to improve the cooperative sensing performance. Assuming $P(H_0)$ and $P(H_1)$, two attack parameters α and β are simultaneously estimated. The estimation of attack parameters is based on the value of received sensing reports. Two parameters m and v are defined as:

$$m = \frac{1}{N}\sum_{j=1}^{N} E_j, \quad v = \frac{1}{N}\sum_{j=1}^{N} {E_j}^2 \tag{16}$$

The mathematical expectation of m and v are:

$$E(m) = \frac{1}{N}\sum_{j=1}^{N} E(E_j), \quad v = \frac{1}{N}\sum_{j=1}^{N} E({E_j}^2) \tag{17}$$

By considering four different hypotheses $H_{s_0}, H_{s_1}, H_{s_2}$ and H_{s_3} we have:

$$\begin{aligned} E(E_j) =& E(E_j|H_{s_0})\pi_0 + E(E_j|H_{s_1})\pi_1 \\ &+ E(E_j|H_{s_2})\pi_2 + E(E_j|H_{s_3})\pi_3 \\ =& \mu_0\pi_0 + \mu_1\pi_1 + \mu_2\pi_2 + \mu_3\pi_3 \\ =& M\pi_0 + M(\gamma_j + 1)\pi_1 + M(\lambda_j + 1)\pi_2 \\ &+ M(\gamma_j + \lambda_j + 1)\pi_3 \end{aligned} \tag{18}$$

Accordingly,

$$\begin{aligned} E({E_j}^2) =& (\mu_0^2 + \sigma_0^2)\pi_0 + (\mu_1^2 + \sigma_1^2)\pi_1 \\ &+ (\mu_2^2 + \sigma_2^2)\pi_2 + (\mu_3^2 + \sigma_3^2)\pi_3 \\ =& (M^2 + 2M)\{\pi_0 + (\gamma_j + 1)^2\pi_1 \\ &+ (\lambda_j + 1)^2\pi_2 + (\gamma_j + \lambda_j + 1)^2\pi_3\} \end{aligned} \tag{19}$$

Obviously, two Equations (18) and (19) are the mean and second-order moment values of received sensing reports, respectively. Finally, by substituting Equations (18) and (19) into Equation (17), two parameters $E(m)$ and $E(v)$ are calculated as:

$$\begin{aligned} E(M) =& M\pi_0 + M(\bar{\gamma} + 1)\pi_1 + M(\bar{\lambda} + 1)\pi_2 \\ &+ M(\bar{\gamma} + \bar{\lambda} + 1)\pi_3 \end{aligned} \tag{20}$$

and

$$\begin{aligned} E(v) =& (M^2 + 2M)\{\pi_0 + (2\bar{\gamma}^2 + 2\bar{\gamma} + 1)\pi_1 \\ &+ (2\bar{\lambda}^2 + 2\bar{\lambda} + 1)\pi_2 \\ &+ (2\bar{\gamma}^2 + 2\bar{\lambda}^2 + 2\bar{\gamma}\bar{\lambda} + 2\bar{\gamma} + 2\bar{\lambda} + 1)\pi_3\} \end{aligned} \tag{21}$$

where $\bar{\gamma} = \frac{1}{N}\sum_{j=1} N\gamma_j$ is the average SNR between PU and CR users and $\bar{\lambda} = \frac{1}{N}\sum_{j=1} N\lambda_j$ is also the average SNR between PUEA and CR users. Regarding to exponential distribution of γ_j and λ_j , $E({\gamma_j}^2) = 2\bar{\gamma}^2$ and $E({\lambda_j}^2) = 2\bar{\lambda}^2$. By substituting the Equation (2) in Equations (20) and (21), these equations can be summarized as:

$$\begin{cases} \psi_0\alpha + \psi_1\beta = \phi_0 \\ \psi_2\alpha + \psi_3\beta = \phi_1 \end{cases} \tag{22}$$

where the parameters $\psi_0, \psi_1, \psi_2, \psi_3, \phi_0$ and ϕ_1 are defined as:

$$\begin{aligned} &\psi_0 = P(H_1)M\bar{\lambda} \\ &\psi_1 = P(H_0)M\bar{\lambda} \\ &\psi_2 = (2M + M^2)P(H_1)(\bar{\gamma} + \bar{\lambda} + 1)2\bar{\lambda} \\ &\psi_3 = (2M + M^2)P(H_0)(\bar{\lambda} + 1)2\bar{\lambda} \\ &\phi_0 = E(m) - M[P(H_0) + P(H_1)(\bar{\gamma} + 1)] \\ &\phi_1 = E(v) - (2M + M^2)[(P(H_0) + P(H_1)) \\ &\quad (2\bar{\gamma}^2 + 2\bar{\gamma} + 1)] \end{aligned}$$

From the Equation (22), the values of unknown attack parameters α and β are obtained as:

$$\hat{\alpha} = \frac{\psi_1\phi_1 - \psi_3\phi_0}{\psi_1\psi_2 - \psi_0\psi_3} \quad \hat{\beta} = \frac{\psi_2\phi_0 - \psi_0\phi_1}{\psi_1\psi_2 - \psi_0\psi_3}$$
$$\psi_1\psi_2 \neq \psi_0\psi_3 \quad (\gamma \neq 0) \tag{23}$$

The proposed ACSS approach is based on LLRT method. Two attack parameters α and β are estimated and then used in the LLRT hypothesis testing.

Two conditional PDFs of decision statistics Y are expressed as follows:

$$\begin{aligned} p(Y|H_1) =& p(Y|H_1, E^{on})P(E^{on}|H_1) \\ &+ p(Y|H_1, E^{off})P(E^{off}|H_1) \\ p(Y|H_0) =& p(Y|H_0, E^{on})P(E^{on}|H_0) \\ &+ p(Y|H_0, E^{off})P(E^{off}|H_0) \end{aligned} \tag{24}$$

With regard to $\alpha = P(E^{on}H_1)$ and $\beta = P(E^{on}H_0)$, we have:

$$\begin{aligned} p(Y|H_1) = p(Y|H_1, E^{on})\alpha + p(Y|H_1, E^{off})(1 - \alpha) \\ p(Y|H_0) = p(Y|H_0, E^{on})\beta + p(Y|H_0, E^{off})(1 - \beta) \end{aligned} \tag{25}$$

Thus, the decision statistic of the LLRT scheme, expressed in Equation (10) can be generalized by the following formula:

$$\begin{aligned} \Lambda =& log\left(\frac{p(Y|H_1)}{p(Y|H_0)}\right) \\ =& log\left(\frac{p(Y|H_1, E^{on})\alpha + p(Y|H_1, E^{off})(1 - \alpha)}{p(Y|H_0, E^{on})\beta + p(Y|H_0, E^{off})(1 - \beta)}\right) \\ =& log\left(\frac{p(Y|H_{s_3})\alpha + p(Y|H_{s_1})(1 - \alpha)}{p(Y|H_{s_2})\beta + p(Y|H_{s_0})(1 - \beta)}\right) \underset{H_0}{\overset{H_1}{\gtrless}} \eta \end{aligned} \tag{26}$$

It should be noted that the above equation for $\alpha = \beta = 0$ is the same as Equation (10).

4 Simulation Results and Discussions

We provide numerical simulations to demonstrate the advantage of our proposed ACSS scheme in the presence of a malicious PUEA. In the proposed system model the channel is assumed to be Rayleigh fading and there are 12 CR users ($N = 12$) that use energy detection by $M = 30$ sample in a detection interval. The prior probabilities $P(H_0)$ and $P(H_1)$ are assumed to be 0.8 and 0.2, respectively. The global threshold η is selected as $log(P(H_0))/P(H_1))$. All parameters are constant unless otherwise specified.

Results are obtained through Monte-Carlo simulations over 104 runs. Throughout the simulations, we have labeled the curves by "LLRT (No Attach)" when there is not any PUEA signals and labeled them by "Conventional LLRT" in the case that there is PUEA signals but the FC is not aware of the fake signals.

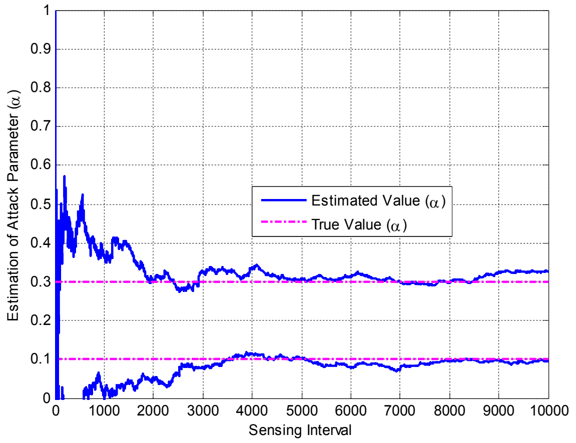

Figure 2. The convergence of attack parameter ($\alpha = 0.1, 0.3$)

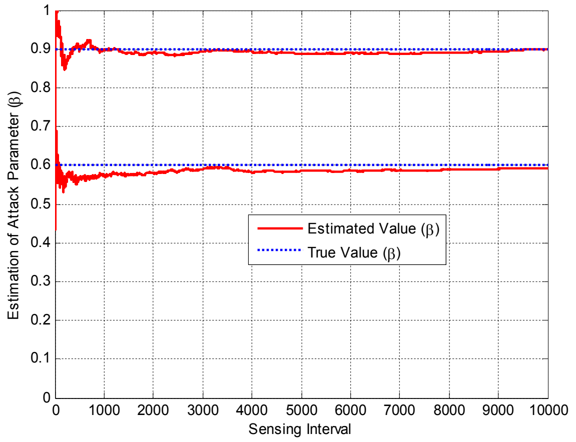

Figure 3. The convergence of attack parameter ($\beta = 0.6, 0.9$)

Figures 2 and 3 show the convergences of attack parameters for $\alpha = 0.1, 0.3$ and $\beta = 0.6, 0.9$, respectively. The estimated values for α and β are converged to constant values after applying almost 1000 and 3000 rounds of sensing, respectively. Regarding the value of $P(H_1)$ and $\alpha = 0.3$ meaning that the PUEA transmits the fake signal only in 30% of hypothesis H_1, the convergence of α happens later than that of β . In the simulation, the initial stage can be set as the first 3000 sensing intervals where the attack parameters are estimated and then used to find optimum thresholds to improve the CSS process in the presence of a malicious PUEA.

Figures 4, 5, and 6 show the correct sensing probabilities versus SNR $(\bar{\gamma})$ for attack strength 0.1, 0.5 and 1, respectively. As shown in the figures, using the proposed ACSS method improves the performance of CSS under malicious PUEA signals. As for $\rho = 0.1$, where the PU is 10 times more powerful than the PUEA, the effect of the attacker is negligible and increasing two attack parameters α and β has no effect on correct sensing probability. For $\rho = 0.5$ and $\rho = 1$, as

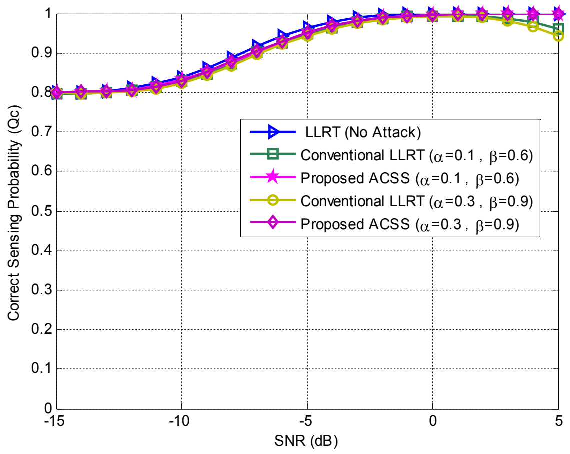

Figure 4. Probability of correct sensing versus average SNR (γ) with $\rho = 0.1$

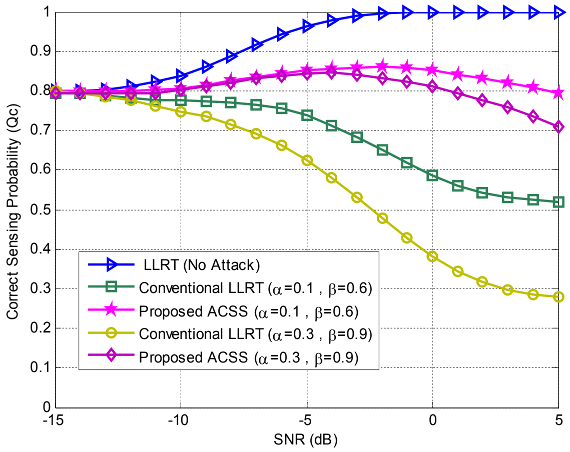

Figure 5. Probability of correct sensing versus average SNR (γ) with $\rho = 0.5$

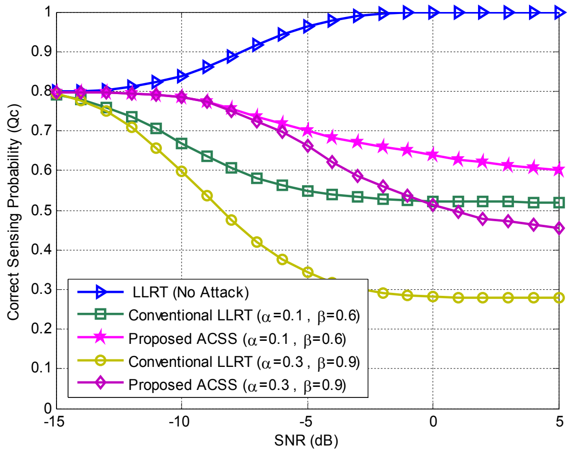

Figure 6. Probability of correct sensing versus average SNR (γ) with $\rho = 1$

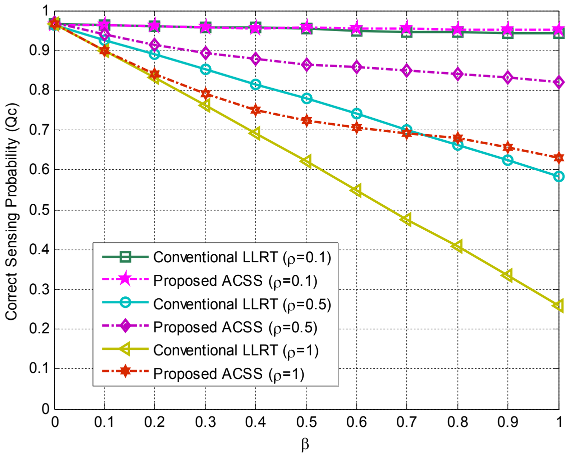

Figure 7. Probability of correct sensing versus β with SNR=-5dB and $\alpha = 0.1$

shown in Figures 5 and 6, using the proposed method remarkably improves performance of CSS under fake signals of the PUEA. In addition, as α and β increase, improvement gained by our proposed method will increase. For $\alpha = 0.3, \beta = 0.9$, the difference between conventional and proposed method is greater than for $\alpha = 0.1, \beta = 0.6$. It should be noted that in both spectrum sensing procedures (conventional and proposed) the PUEA can decrease the probability of correct sensing at the FC by increasing parameters α and β.

Figure 7 depicts the correct sensing probability versus attack parameter β for various attack strength $\rho(0.1, 0.5, 1)$ in SNR=-5dB and $\alpha = 0.1$. As shown in the figure, in conventional method, increasing both parameters ρ and β leads to less correct sensing probability, in contrary, by the proposed ACSS method, increasing ρ and β causes a small change in the rate of correct sensing probability.

Figures 8 and 9 depict the 3-D plot of correct sensing probabilities versus α and β for conventional and proposed ACSS methods, respectively. The average SNR $(\bar{\gamma})$ and attack strength (ρ) are assumed to be -5 dB and 0.5, respectively. As shown, in conventional method, with increasing α and β the correct sensing probability is remarkably decreased. Using the proposed ACSS method high gain is achieved, where for $\alpha = \beta = 1$, in which the PUEA is always present, the correct sensing probability reduces to 0.9.

The results obtained from Figures 10 and 11 for $\rho = 1$ are also similar to that of Figures 8 and 9, respectively.

In Figures 12 and 13, the attack strength ρ is assumed to be 2, where a powerful PUEA is considered, it is concluded that the proposed method is even useful for $\rho > 1$.

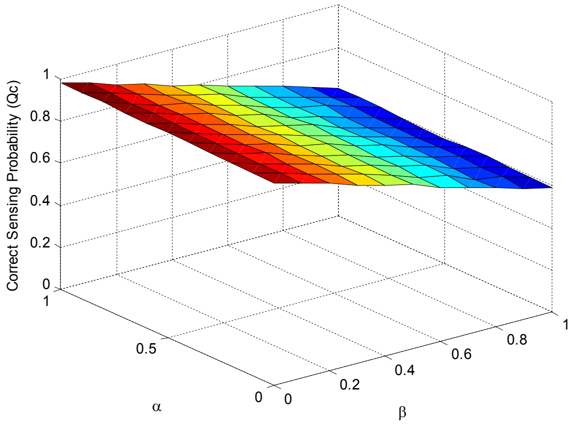

Figure 8. Probability of correct sensing versus α, β with $\rho = 0.5$ for conventional method

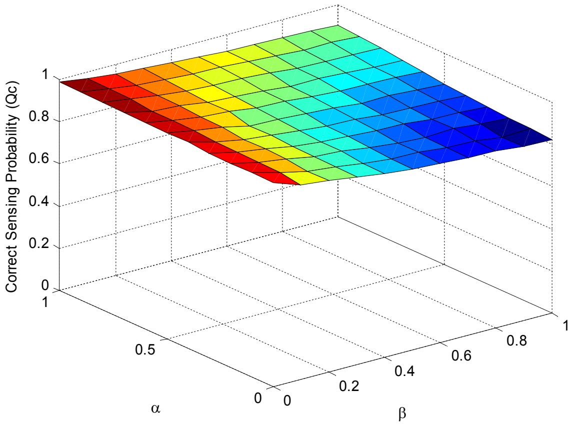

Figure 9. Probability of correct sensing versus α, β with $\rho = 0.5$ for proposed ACSS scheme

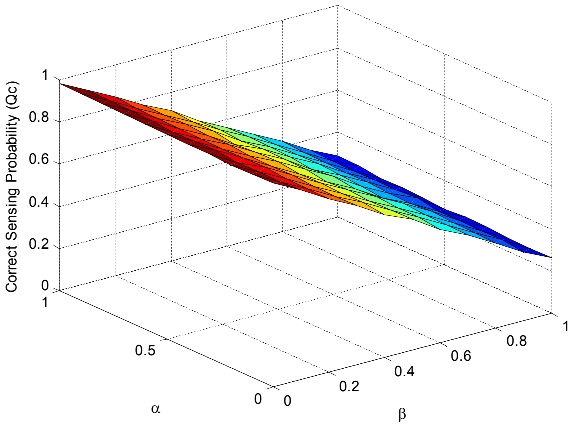

Figure 10. Probability of correct sensing versus α, β with $\rho = 1$ for conventional method

5 Conclusion

In the current study, Cooperative Spectrum Sensing (CSS) in the presence of Primary User Emulation Attack (PUEA) was investigated. As a countermeasure against PUEA, an appropriate defense strategy was

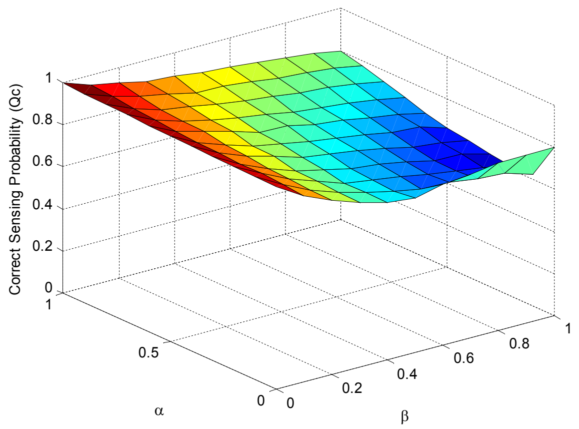

Figure 11. Probability of correct sensing versus α, β with $\rho = 1$ for proposed ACSS scheme

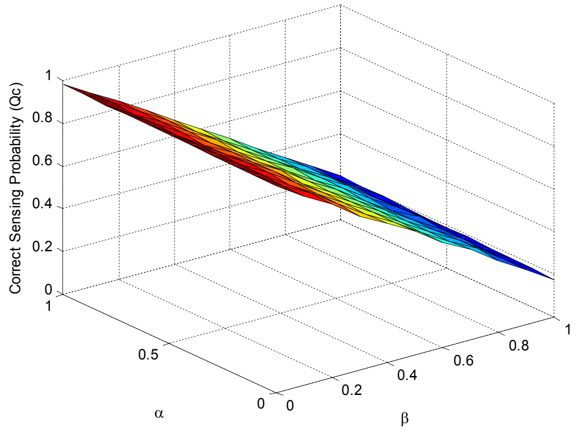

Figure 12. Probability of correct sensing versus α, β with $\rho = 1$ for conventional method

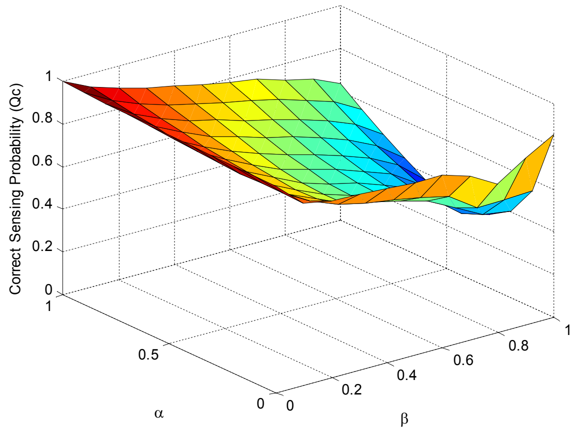

Figure 13. Probability of correct sensing versus α, β with $\rho = 1$ for proposed ACSS scheme

proposed which estimated two attack parameters, *i.e.* probabilities of the presence of a PUEA fake signal in occupied and unoccupied frequency bands, and applied to Log-Likelihood Ratio Test (LLRT) to determine the hold hypothesis. We observed that when the average SNR in CR users received from PU and PUEA are identical, neither CR users nor the FC can differentiate between received signal from PU and PUEA. In this case, the proposed method improved the CSS performance. The obtained results verified the effectiveness of the proposed scheme compared with conventional method.

References

[1] J. Mitola and G. Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6(4):13–18, Aug 1999. ISSN 1070-9916. doi: 10.1109/98.788210.

[2] S. Haykin. Cognitive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 23(2):201–220, Feb 2005. ISSN 0733-8716. doi: 10.1109/JSAC.2004.839380.

[3] Ian F. Akyildiz, Won-Yeol Lee, Mehmet C. Vuran, and Shantidev Mohanty. Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey. *Computer Networks*, 50(13):2127 – 2159, 2006. ISSN 1389-1286. doi: http://dx.doi.org/10.1016/j.comnet.2006.05.001. URL `http://www.sciencedirect.com/science/article/pii/S1389128606001009`.

[4] S. M. Mishra, A. Sahai, and R. W. Brodersen. Cooperative sensing among cognitive radios. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 4, pages 1658–1663, June 2006. doi: 10.1109/ICC.2006.254957.

[5] Ian F. Akyildiz, Brandon F. Lo, and Ravikumar Balakrishnan. Cooperative spectrum sensing in cognitive radio networks: A survey. *Physical Communication*, 4(1):40 – 62, 2011. ISSN 1874-4907. doi: http://dx.doi.org/10.1016/j.phycom.2010.12.003. URL `http://www.sciencedirect.com/science/article/pii/S187449071000039X`.

[6] R. Chen and J. M. Park. Ensuring trustworthy spectrum sensing in cognitive radio networks. In *Networking Technologies for Software Defined Radio Networks, 2006. SDR '06.1st IEEE Workshop on*, pages 110–119, Sept 2006. doi: 10.1109/SDR.2006.4286333.

[7] S. Anand, Z. Jin, and K. P. Subbalakshmi. An analytical model for primary user emulation attacks in cognitive radio networks. In *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*, pages 1–6, Oct 2008. doi: 10.1109/DYSPAN.2008.16.

[8] R. Chen, J. M. Park, and J. H. Reed. Defense against primary user emulation attacks in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 26(1):25–37, Jan

2008. ISSN 0733-8716. doi: 10.1109/JSAC.2008.080104.

[9] Z. Yuan, D. Niyato, H. Li, J. B. Song, and Z. Han. Defeating primary user emulation attacks using belief propagation in cognitive radio networks. *IEEE Journal on Selected Areas in Communications*, 30(10):1850–1860, November 2012. ISSN 0733-8716. doi: 10.1109/JSAC.2012.121102.

[10] C. Chen, H. Cheng, and Y. D. Yao. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. *IEEE Transactions on Wireless Communications*, 10(7):2135–2141, July 2011. ISSN 1536-1276. doi: 10.1109/TWC.2011.041311.100626.

[11] Abbas Ali Sharifi, Morteza Sharifi, and Mir Javad Musevi Niya. Collaborative spectrum sensing under primary user emulation attack in cognitive radio networks. *IETE Journal of Research*, 62 (2):205–211, 2016. doi: 10.1080/03772063.2015.1083907. URL `http://dx.doi.org/10.1080/03772063.2015.1083907`.

[12] Abbas Ali Sharifi, Morteza Sharifi, and Mir Javad Musevi Niya. Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach. {*AEU*} - *International Journal of Electronics and Communications*, 70(1):95 – 104, 2016. ISSN 1434-8411. doi: http://dx.doi.org/10.1016/j.aeue.2015.10.010. URL `http://www.sciencedirect.com/science/article/pii/S1434841115003106`.

[13] Maryam Haghighat and Seyed Mohammad Sajad Sadough. Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users. {*AEU*} - *International Journal of Electronics and Communications*, 68(6):520 – 527, 2014. ISSN 1434-8411. doi: http://dx.doi.org/10.1016/j.aeue.2013.12.010. URL `http://www.sciencedirect.com/science/article/pii/S143484111300318X`.

[14] M. Haghighat and S.M.S. Sadough. Smart primary user emulation in cognitive radio networks: defence strategies against radio-aware attacks and robust spectrum sensing. *Transactions on Emerging Telecommunications Technologies*, 26 (9):1154–1164, 2015. ISSN 2161-3915. doi: 10.1002/ett.2848. URL `http://dx.doi.org/10.1002/ett.2848`.

[15] J. Ma, G. Zhao, and Y. Li. Soft combination and detection for cooperative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 7(11):4502–4507, November 2008. ISSN 1536-1276. doi: 10.1109/T-WC.2008.070941.

[16] H. Urkowitz. Energy detection of unknown deterministic signals. *Proceedings of the IEEE*, 55 (4):523–531, April 1967. ISSN 0018-9219. doi: 10.1109/PROC.1967.5573.

[17] F. F. Digham, M. S. Alouini, and M. K. Simon. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communications*, 55(1):21–24, Jan 2007. ISSN 0090-6778. doi: 10.1109/TCOMM.2006.887483.

[18] Athanasios Papoulis and S Unnikrishna Pillai. *Probability, Random variables, and Stochastic Processes.* Tata McGraw-Hill Education, 4 edition, 2006.

[19] Pramod K. Varshney. *Distributed Detection and Data Fusion.* Springer New York, 1997. ISBN 978-1-4612-1904-0. doi: 10.1007/978-1-4612-1904-0. URL `http://dx.doi.org/10.1007/978-1-4612-1904-0`.

Abbas Ali Sharifi received the B.Sc. degree in electronic engineering from Amirkabir University of Technology, and the M.Sc. and Ph.D. degrees in telecommunication engineering from Malek Ashtar University of Technology and University of Tabriz, respectively. His current research interests include wireless communication and networking, cognitive radio, security, and energy harvesting.

Javad Musevi Niya received his B.S. degree from University of Tehran, his M.S. degree from Sharif University of Technology and his Ph.D. degree in Electrical Engineering from University of Tabriz. He is working as an academic member of the Faculty of Electrical and Computer Engineering, University of Tabriz. His research interests are wireless communication systems and signal processing.